

REMARKS

Reconsideration of the present application, as amended, is respectfully requested. Claims 1, 2, 14, and 17 have been amended. Therefore, claims 1-31 are presented for examination.

In the Advisory Action, the Examiner entered the claims, but noted that he still had the same issues with the claims. Applicants have amended the claims to further clarify the invention.

Claims 1-31 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. The Examiner suggested that the limitations of "the record ID being a random record ID generated for tracking authentication data" is not enabled by the Specification. Applicants respectfully disagree. In particular, page 14, lines 7-13 state "For one embodiment, database 510 includes a client ID, or record ID 515, which identifies the client. For one embodiment, the client ID 515 is randomly generated at the time the client registers with the authentication server 220." Note that the record ID is randomly generated once, when the user registers with the authentication server. This record ID is then consistently used for that user. The point of such a record ID is to dissociate the user's identity information (i.e. user name, email address, etc.) from the user's authentication information (i.e. biometric data, password, etc.). This provides additional security, in that even if the authentication database is compromised, it is not possible to identify the individual whose authentication data is obtained.

Applicants have further clarified this, for example in claim 1, by amending the claim to read "the record ID being a random number generated for tracking

authentication data and disassociating the authentication data from other client identity data." Thus, it should be clear that the record ID is consistent, used to identify the user, and randomly generated. If the Examiner still has issues with the "random" aspect, the Examiner is asked to contact the undersigned with further suggestions on how to amend the claims to clarify this distinction.

Claims 1-6, 8, 9, 11-14, 17, 20-24, 26, 27 and 29-31 remain rejected under 35 U.S.C. §103(a) over U.S. Patent 6,853,988 to Dickenson, et al. in view of U.S. Patent 6,006,334 to Nguyen, et al.

As previously discussed, Dickinson does not teach or suggest the use of a record ID to track authentication data. The Examiner notes that Dickinson does not teach or suggest associating authentication data with a record ID. The Examiner suggests that Nguyen teaches this element.

The Examiner appears to misunderstand Nguyen. Nguyen's system is designed to detect two users attempting to access the same resource with the same user name and password. The "random number" associated with the password is simply used to disambiguate between multiple users of the same password. Nguyen creates no relationship between a authentication data and a record ID. The Examiner suggests that Nguyen, column 4, line 64 to column 5, line 23 teaches this. However, the referenced section of Nguyen states:

Referring to FIG. 2, the Authenticate operation of Table 1 is illustrated. A User 200 Authenticates to a lobby server 220 with cookie 210 (as used herein, cookie means a password plus some additional random factor such as, for example, a random number, a time stamp, or an alpha-numeric string). The lobby server 220 will then check that the cookie contains a valid password (passwords have been purchased and are stored at the central database to designate valid users), as illustrated in

the flowchart of FIG. 3. It is first determined at decision block 300 whether or not the password is valid. If not, the password is rejected at block 390. If the password is valid, it is determined at decision block 320 whether or not a user record exists for this user. If the response to decision block 320 is no, the lobby server 220 (see FIG. 2) will create a User Record for that password at block 350. Once the record is completed, the present invention returns success at 380. If the response to decision block 320 is yes, it is determined at block 325 whether or not the cookie provided by the user matches that in the User Record. If the response to decision block 325 is yes, then the process returns success at block 380. If the response to decision block 325 is no, it is determined at decision block 330 whether or not visiting server is null. If the response to decision block 330 is no, the present invention invokes a Duplication Handler at block 352. If the response to decision block 330 is yes, the cookie in the User Record is replaced at block 340 and success is indicated at 380.

As can be seen the "random factor" of Nguyen is a one-time randomizer used to disambiguate log-ins with the same password and user ID. This is further clarified in Nguyen, when it states, in claim 1:

- creating a user record containing the user identification, the password and the initial random factor;
- receiving a subsequent request to access the distributed service utilizing the user identification, the password and a subsequent random factor;
- accessing the user record corresponding to the user identification of the subsequent request; and
- restricting use of the distributed service to said user during a subsequent request to access the distributed service with said user identification based on the accessed user identification, the password and said initial random factor contained in the user record.

As can be seen, the "random factor" of Nguyen is not a consistent record ID, but rather a disambiguation for differentiating between attempted log-ins. There is absolutely no mention in Nguyen of associating authentication data with a record ID. Nguyen does not use the random number as a record ID at all.

Claim 1 recites in part "receiving a record ID for a user, the record ID being a random number generated for tracking authentication data and disassociating the

authentication data from other client identity data." As noted above, neither Dickinson nor Nguyen teach or suggest a record ID being a random number used for tracking authentication data and for disassociating the authentication data from other client identity data. Therefore, claim 1, and claims 2-13 which depend on it, are not obvious over Dickinson in view of Nguyen.

Claim 14 similarly recites "looking up a record ID associated with the user, the record ID being a random number generated to track the user's authentication data and used to separate the user's other identity information from the authentication data." As noted above, neither Dickinson nor Nguyen teach or suggest a record ID to separate user's identity from authentication data. Therefore, claim 14, and claims 15-16 which depend on it, are not obvious over Dickinson in view of Nguyen.

Claim 17 similarly recites in part: "the record ID being a randomly generated number used to separate the user's other identity information from the user's authentication data." As noted above, neither Dickinson nor Nguyen teach or suggest a record ID randomly generated to separate the user's identity from authentication data. Therefore, claim 17, and claims 18-31 which depend on it, are not obvious over Dickinson in view of Nguyen

Claims 7, 10, 25 and 28 were rejected under 35 U.S.C. §103(a) over U.S. Patent 6,853,988 to Dickenson, et al. and U.S. Patent 6,006,334 to Nguyen, et al. and in further view of U.S. Patent 6,581,161 to Byford.

Byford teaches the use of biometric data for authentication. However, Byford does not teach or suggest the use of a record ID in this context. Therefore, Byford does

not overcome the shortcomings of Dickinson and Smith discussed above. Thus, claims 7, 10, 25, and 28 are not obvious over Dickinson in view of Byford.

Claims 15, 16, 18 and 21 were rejected under 35 U.S.C. §103(a) over U.S. Patent 6,853,988 to Dickenson, et al. and U.S. Patent 6,006,334 to Nguyen, et al. and in further view of U.S. Patent 5,695,106 to Towers et al.

Towers discusses the determination of authentication policy associated with a user. However, Towers does not teach or suggest the use of a record ID in this context. Therefore, Towers does not overcome the shortcomings of Dickinson and Nguyen discussed above. Thus, claims 15, 16, 18 and 21 are not obvious over Dickinson in view of Nguyen, further in view of Towers.

Claims 19 and 22 were rejected under 35 U.S.C. §103(a) over U.S. Patent 6,853,988 to Dickenson, et al. and U.S. Patent 6,006,334 to Nguyen, et al. and in further view of U.S. Patent 6,119,227 to Mao.

Mao discusses nonce generation to be included with user authentication data. However, Mao does not teach or suggest the use of a record ID in this context. Therefore, Mao does not overcome the shortcomings of Dickinson and Nguyen discussed above. Thus, claims 19 and 22 are not obvious over Dickinson in view of Nguyen, further in view of Mao.

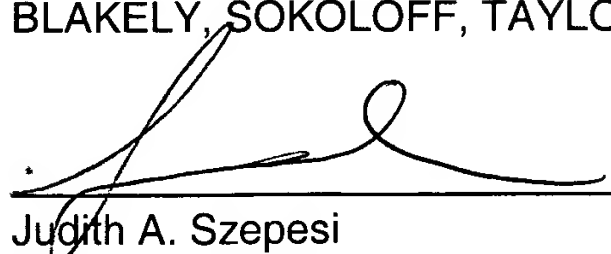
Applicant respectfully submits that in view of the amendments and discussion set forth herein, the applicable rejections have been overcome. Accordingly, the present and amended claims should be found to be in condition for allowance.

If a telephone interview would expedite the prosecution of this application, the Examiner is invited to contact Judith Szepesi at (408) 720-8300.

If there are any additional charges/credits, please charge/credit our deposit
account no. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 3/14, 2006


Judith A. Szepesi
Reg. No. 39,393

Customer No. 08791
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300